Section 2 (U) General Investigative and Administrative Activities and Requirements

2-01 (U) General Investigative and Administrative Activities and Requirements

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-02 (U) NATIONAL SECURITY INVESTIGATIONS

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-03 (U) SUMMARY GUIDANCE AND APPLICABILITY OF THREAT ASSESSMENTS:

(S)

b1

(S)

b1

B. (U) Retention of Threat Assessment Information

1. The NSIG authorize, with certain limitations, the retention and dissemination of threat assessment information for broad analytic and intelligence purposes, regardless of whether it furthers investigative objectives in a narrower or more immediate sense. Accordingly, even if information obtained during a Threat Assessment does not warrant opening either a Preliminary Investigation or a Full Investigation, those who possess personally identifying information derived from Threat Assessments may retain it for valid national security purposes. In that regard, the information may eventually serve a variety of valid analytic purposes as pieces of the overall intelligence picture are connected to thwart terrorist activities. In addition, the information may possibly assist FBI personnel in responding to any questions which may subsequently arise as to the nature and extent of the Threat Assessment and its results, whether positive or negative.

2. One cautionary point in this regard must be emphasized. This type of information, i.e., information obtained during a Threat Assessment that has insufficient value to justify further investigative activity (at least at the time it is obtained), is often sensitive personal information concerning U.S. persons and entities. If it is retained for the purposes addressed above, measures should be taken to identify it accurately as Threat Assessment information, to protect it from inadvertent disclosure, and to preclude its use as a basis for any further investigative activity unless and until such action is authorized by the NSIG or other applicable regulations.

2-04 (U) SUMMARY GUIDANCE AND APPLICATION FOR PRELIMINARY INVESTIGATIONS (PI)

(S)

b1

B. (U) Sensitive National Security Matters. A PI initiated by a field office that involves a Sensitive National Security Matter may be approved by a SAC. b7E

1. A *Sensitive National Security Matter as defined in the NSIG is a threat to the national security involving* [redacted] *a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials.*

(S) [redacted] b1

(U) D. (X) All Sensitive National Security Matters not specifically mentioned above may be approved by the SAC, but may not be delegated.

(U) E. (X) PIs not involving Sensitive National Security Matters may be approved by an SAC or as authorized by the SAC, the ASAC or squad supervisor with national security investigative responsibility.

(S) [redacted] b1

(S) [redacted] b1

cooperative witnesses)
Recruitment

(S) [redacted] b1

[redacted] b1 Referral/Consult

5. Undercover Operations (UC): (*Discussed in Section 28*)

a. Group I UC operations involving *Sensitive Circumstances* necessitate the following requirements:

(U) [redacted] b7E

b. Group II UC operations necessitate the following requirements:

(S) [redacted] b1

1. SAC Approval

(S)

b1

6. Undisclosed participation (UDP):
UDP is defined as the joining or participating in the activities of an organization by an FBI asset or employee without disclosure of FBI affiliation, but not including participation with the knowledge and approval of an official of the organization authorized to act in relation to the activities in question, attendance at an activity open to the public or to acknowledged U.S. Government employees, personal activities not related to FBI employment, or attendance at an academic institution to obtain education or training relevant to FBI employment or to a future undercover role. The UDP policy contained in this Manual applies to investigations conducted pursuant to the NSIG.

Executive Order 12333, Part 2.9, (EO) permits undisclosed participation "in accordance with procedures established by the head of the agency concerned and approved by the Attorney General" The EO provides two substantive requirements. First, UDP must be "essential to achieving lawful purposes," as determined by the agency head, i.e., the Director of the FBI. Second, UDP cannot be undertaken for the purpose of influencing the activity of the organization or its members, unless undertaken on behalf of the FBI in the course of a lawful investigation, or the organization concerned is composed primarily of individuals who are not U.S. Persons and is reasonably believed to be acting on behalf of a foreign power.
a. It should be noted that not all UDP constitutes an undercover operation. Similarly, approvals for UDP do not alleviate the need for review of undercover activities by the undercover review committees.

b. "Organization" refers generally to any association of two or more persons and is to be interpreted broadly.

c. The "participant" in UDP may be a special agent or other employee of the FBI, or a source recruited for the purpose of obtaining information.

(S)

b1
Referral/Consult

b1
Referral/Consult

(S)

5. Undercover Operations (UC): (*Discussed in Section 28*)

b7E

b. Group II UC operations

i. APPROVAL AUTHORITY FOR UDP IN NATIONAL SECURITY INVESTIGATIONS:

b7E

[redacted]

b7E

ii. CRITERIA FOR APPROVAL OF UDP

[redacted]

b7E

7. Mail Cover

i. A "mail cover" is the recording of data appearing on the outside cover of sealed mail matter or of the contents of any unsealed class of mail. A "recording" is a transcription, photograph, photocopy of any other facsimile of the image of the outside cover, envelope, wrappers, or contents of any class of mail. Mail covers are governed by United States Postal Regulations. (See 39 CFR § 233.3)

ii. A request for a national security mail cover [redacted] (See Section Mail Cover at 2-21) b7E

8. Physical and Photographic Surveillance (where such surveillance does not require unconsented entry). This technique includes the use of such surveillance to identify an individual in contact with the subject of a PI. Such surveillance must be approved by the SAC or SAC's designee (ASAC or national security squad supervisor). (See Section 2-09)

9. Video Surveillance of areas which would not require a warrant for law enforcement purposes. When approved by the SAC, the FBI may surveil open public areas where there is no reasonable expectation of privacy. (See Section 2-09)

10. Physical Searches of personal or real property under circumstances in which a warrant would not be required for law enforcement purposes and in which there is no reasonable expectation of privacy (e.g., trash cover. Such physical searches require approval) may be approved by the SAC or the SAC's designee (ASAC or national security squad supervisor may approve).

11. Closed circuit television (CCTV), direction finders, and other monitoring devices under circumstances in which there is no reasonable expectation of privacy and a warrant would not be required for law enforcement purposes (non-trespassory access). Such techniques may be approved by the SAC or ASAC, with CDC or Office of General Counsel review. (See Electronic Surveillance Section for guidance on use of techniques where Privacy Issues attach.)

12. Consensual monitoring of communications (to include consensual computer monitoring). Monitoring of communications to which one of the participants is a consenting party may be approved by SAC or ASAC, with CDC or Office of General Counsel review.

13. Polygraph examinations (See MIOG Part II § 13-22 for policy)

14. National Security Letters (NSL). An NSL is an administrative demand for documents or records which can be made by the FBI in support of national security investigations. There are presently three statutory categories (financial institution records, consumer credit agency records, and electronic communication service provider records) with seven variations of these three NSL types:

[redacted] b7E

15. Accessing stored wire and electronic communications and transactional records in conformity with chapter 121 of Title 18, U.S.C. § 2701-2712.

16. Use of pen registers and trap and trace devices in conformance with Title 50, U.S.C. §§ 1841 - 1846 (FISA), or Title 18, U.S.C. §§ 3121 –3127 (Criminal).

17. Obtaining business records and other tangible things in conformity with Title 50, U.S.C. §§ 1861 - 1863 (FISA).

18. Use of federal grand jury subpoenas and other subpoena authority as may be permitted by law (to include administrative subpoenas where applicable).

2-05 (U) SUMMARY GUIDANCE AND APPLICATION FOR FULL INVESTIGATIONS (FI)

(S)

[redacted]

b1

B. (X) Approval of Full Investigations

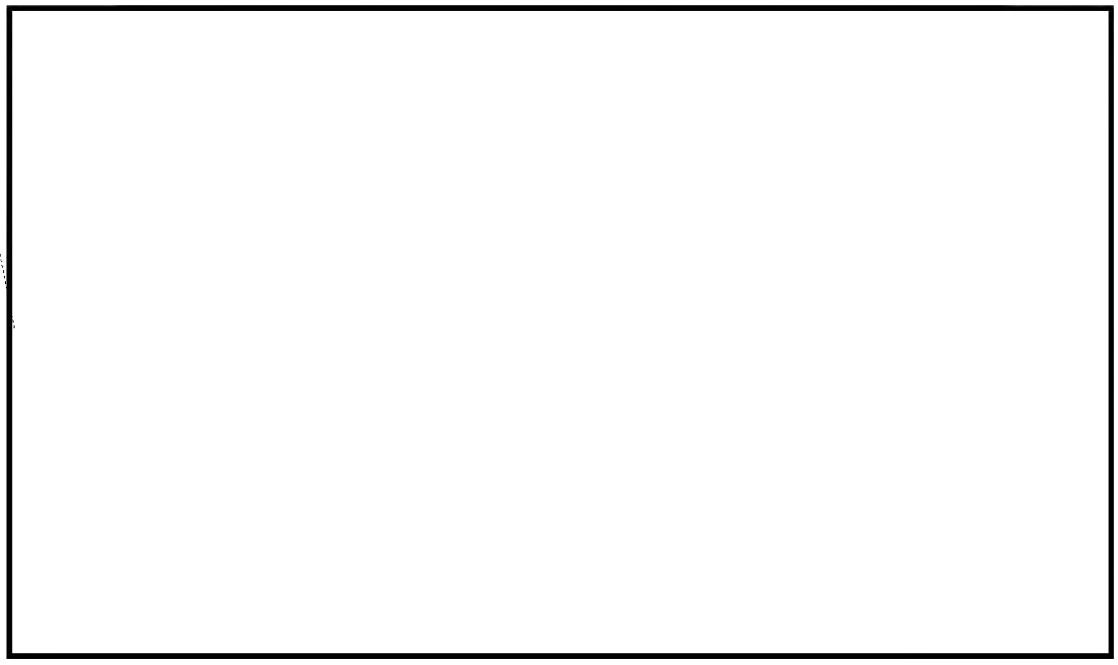
1. An FI initiated by a field office that involves a sensitive national security matter may be approved by an SAC.

b7E

a. *A Sensitive National Security Matter as defined in the NSIG is a threat to the national security involving*

[redacted]

(S)



b1

2-06 (U) Collection of Foreign Intelligence

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-07 (U) Codewords

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-08 (U) Office of Origin

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-09 (U) Physical and Photographic Surveillances

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-10 (U) Interviews In National Security Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-11 (U) Educational Records (Buckley Amendment)

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-12 (U) Polygraph Examinations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-13 (U) Hypnosis

A. (U) See: id. Part II, Section 10-12.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

(MIOG Part 2, Section 10-12 For your information.)

10-12 USE OF HYPNOSIS AS AN INVESTIGATIVE AID

10-12.1 Approval to Utilize (See MIOG, Part 2, 10-3.)

Hypnosis is legally permissible when used as an investigative aid for lead purposes in Bureau cases where witnesses or victims are willing to undergo such an interview. The use of hypnosis should be confined to selective Bureau cases. Upon finding a willing witness or victim, Bureau authority must be obtained from the appropriate Assistant Director (AD) responsible for either the Criminal Investigative Division (CID), the Counterterrorism Division (CTD), or the Counterintelligence Division (CD), who may delegate this

authority to their Section Chief designee. The Critical Incident Response Group's (CIRG's) Behavioral Analysis Unit (BAU) functions as a technical resource to the field and must receive copies of all communications pertaining to the use of hypnosis. Set forth in your request for authorization the name of the hypnosis expert you intend to use and a brief summary of the expert's qualifications. You should consider using a psychiatrist, psychologist, physician, or dentist who is qualified as a hypnotist. Those with forensic training are preferred. If there are no qualified or reliable hypnotists available, the BAU should be contacted to obtain the name of a qualified hypnotist nearest your field division. Upon receipt of Bureau authority, the matter must be thoroughly discussed with the USA. Include the fact that the case Agent or the SAC's designee will attend the hypnotic session, and advise whether that person is likely to participate in the hypnotic session. The use of hypnosis on a witness must have the concurrence of the Assistant United States Attorney (AUSA) in that district, as well as the approval of the AD, CID, CTD, or CD, as appropriate, or their substantive Section Chief designee. You are cautioned that under no circumstances will Bureau personnel participate in hypnotic interviews in non-Bureau cases.

10-12.2 Hypnotic Session

(1) It is recommended that written permission (FD-870) to conduct a hypnotic interview be obtained prior to the interview. This permission should include permission of the witness or victim to have the entire hypnosis session audio or video taped or both.
(2) It is important that you either audio or video tape the entire session and any subsequent hypnotic sessions. Video tape, however, is the preferred method of recording these sessions.
(3) When considering the use of hypnosis, one important aspect is the proper prehypnotic explanation of this technique to the witness or victim. Hypnosis is not a product of the power or magic of the hypnotist. The witness or victim is not likely to reveal his or her innermost secrets or lose control of his or her mind. Further, hypnosis itself is not likely to produce any physical or psychological damage to the person hypnotized.
(4) You must also bear in mind that the use of the information obtained through hypnosis cannot be assumed to be necessarily accurate. Careful investigation is needed to verify the accuracy of information obtained during these sessions.

10-12.3 Role of Case Agent in Hypnotic Session

The case Agent will act as liaison with the hypnotist and will attend the hypnotic session. If the case Agent cannot attend, an SAC-approved designee will handle the duties of the case Agent. It must be clearly understood that the hypnotist is charged with the responsibilities of conducting and supervising the hypnotic session, and must remain physically present throughout the proceedings. With the PRIOR CONCURRENCE AND GUIDANCE of the hypnotist, the case Agent may question the witness or victim under hypnosis, but will not conduct the hypnotic induction or terminate the hypnotic state. The request for authorization to utilize hypnosis will include the name of the case Agent or designee who is acting as liaison. The number of persons actually present at the hypnotic session should be held to a minimum.

10-12.4 Hypnosis Evaluation

In order to evaluate the efficacy of this technique, a detailed summary describing the results of the hypnotic interview must be forwarded to the Bureau with a copy to the Critical Incident Response Group's (CIRG's) Behavioral Analysis Unit (BAU). This summary should specifically include the following items:
(1) The identification of any significant investigative information obtained through the utilization of this technique.
(2) Total number of hypnosis sessions to include the length of each session.

(3) The hypnotic technique utilized to include the manner of recording the interview.
(4) The identity of the case Agent or SAC designee and the hypnotist.
(5) Disposition of the case.

2-14 (U) [redacted]

b7E

Superseded by Corporate olicy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-15 (U) Physical Searches in Which a Warrant is Not Required (Trash Covers)

Superseded by the Domestic Investigations and Operations Guide (DIOG), Section 11.4, dated 12/16/2008

Eff. Date: 12/16/2008

2-16 (U) Monitoring Devices Which Do Not Impose Upon Reasonable Expectations of Privacy

(S) [redacted]

b1

2. Field Office authorization for the use and deployment of these devices may be approved by the SAC or ASAC overseeing National Security Investigations.

C. For circumstances in which there exists a Reasonable Expectation of Privacy and a warrant would be required for law enforcement purposes, see the Electronic Surveillance Section of this manual as it pertains to FISA and Title III electronic surveillance.

2-17 (U) National Security Letters (NSL)

Superseded by the Domestic Investigations and Operations Guide (DIOG), Sections 11.9 and 11.9.3, dated 12/16/2008, and by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

2-18 (U) Deleted

2-19 (U) Business Records

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-20 (U) Deleted

(U) 2-21 ~~(S)~~ Mail Covers

Superseded by the Domestic Investigations and Operations Guide (DIOG), Section 11.3, dated 12/16/2008

Eff. Date: 12/16/2008

2-22 (U) Operations Conducted Outside the United States, the CIA MOU

Superseded by Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-23 (U) The Role of Legal Attaches in Foreign Counterintelligence, Foreign Intelligence and Counterterrorism Investigations (See Legal Attache Manual, Part 1, 6-5.2.2.)

Superseded by Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-24 (U) Otherwise Illegal Activities

A. (U) Otherwise Illegal Activities are actions of FBI employees and Assets which would constitute crimes under Federal, State or local law, but for the fact that they have been officially authorized.

B. (U) Activities which, though illegal, neither violate Federal law nor constitute felonies or serious crimes under State or local law, may be approved by SACs, if the activities are necessary to:

[redacted] b7E

3. Prevent or avoid physical injury to individuals or serious damage to property.

C. (U) All other illegal activities must be approved by FBI Headquarters and, if appropriate the FBI's National Security Undercover Review Committee, after consultation with DOJ's OIPR and the Criminal Division, and the concurrence of the Assistant Attorney General, Criminal Division, or his/her designee.

1. Planned or reasonably foreseeable illegal activities must be approved in advance.

2. In emergency situations however (e.g., when illegal activities are required to prevent death, serious injury, extensive property damage, the loss of significant intelligence information or the compromise of an intelligence operation), senior FBI Headquarters officials may approve them. Under such circumstances, though, the aforestated referrals must be made as soon as possible after the fact. See: Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, CI or IT Intelligence Investigations, Section VII.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

(S) [redacted] b1

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-26 (U) Visa Objections

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-27 (U) Office of Foreign Missions (OFM)

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-28 (U) National Counterintelligence Executive

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-29 (U) Laboratory Assistance

For information regarding the FBI's Laboratory Division and their variety of services, see Laboratory Division's website: [redacted] b7E

2-30 (U) Monitoring of Establishments Program

(S) [redacted] b1

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: ~~Secret~~

2-31 (U) Purchases of Technical Equipment Program

(S) [redacted] b1

(S) [redacted] b1

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: ~~Secret~~

2-32 (U) Blind Faith Program

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

(C) [redacted] b1

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-34 (U) Special Surveillance Group (SSG) Program

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-35 (U) The Behavioral Analysis Program (BAP)

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-36 (U) Investigations of Current and Former Department of State Personnel, and Diplomatic Missions Personnel Abroad

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-37 (U) Investigations of Current and Former Central Intelligence Agency Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-38 (U) Investigations of Current and Former Military and Civilian Department of Defense Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-39 (U) Investigations of Current and Former Department of Energy Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-40 (U) Investigations of Other Government Agency Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-41 (U) Investigations of White House Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-42 (U) Investigations of Presidential Appointees

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-43 (U) Investigations of Members of the Judiciary

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-44 (U) Investigations of Members of the U.S. Congress and their Staffs

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-45 (U) Disseminating Information to Other Agencies in the Federal Government

The following guidance is derived from Section VII. B. of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection of October 31, 2003 ("NSIG"), and it pertains to information obtained under the NSIG. Separate rules apply to information obtained under the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations of May 30, 2002. In addition to the following guidance, it is important to bear in mind that information obtained under the Foreign Intelligence Surveillance Act may only be disseminated in accordance with applicable minimization procedures (See Section 3-06 of this Manual).

Legal rules and Department of Justice policies regarding information sharing and interagency coordination have been significantly modified since the September 11, 2001, terrorist attack by statutory reforms and new Attorney General guidelines. The general principle reflected in current laws and policies is that information should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. Under this general principle, the FBI shall provide information expeditiously to other agencies in the Intelligence Community, so that these agencies can take action in a timely manner to protect the national security in accordance with their lawful functions. This Subpart provides standards and procedures for the sharing and dissemination of information obtained in national security investigations, foreign intelligence collection, and other activities under the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection of October 31, 2003 ("NSIG") (U)

1. General (U) outside U.S.

a. Information may be disseminated with the consent of the person whom the information concerns, or where necessary to protect life or property from

threatened force or violence, otherwise necessary for the safety or security of persons or property or for the prevention of crime, or necessary to obtain information for the conduct of a lawful investigation by the FBI. (U)

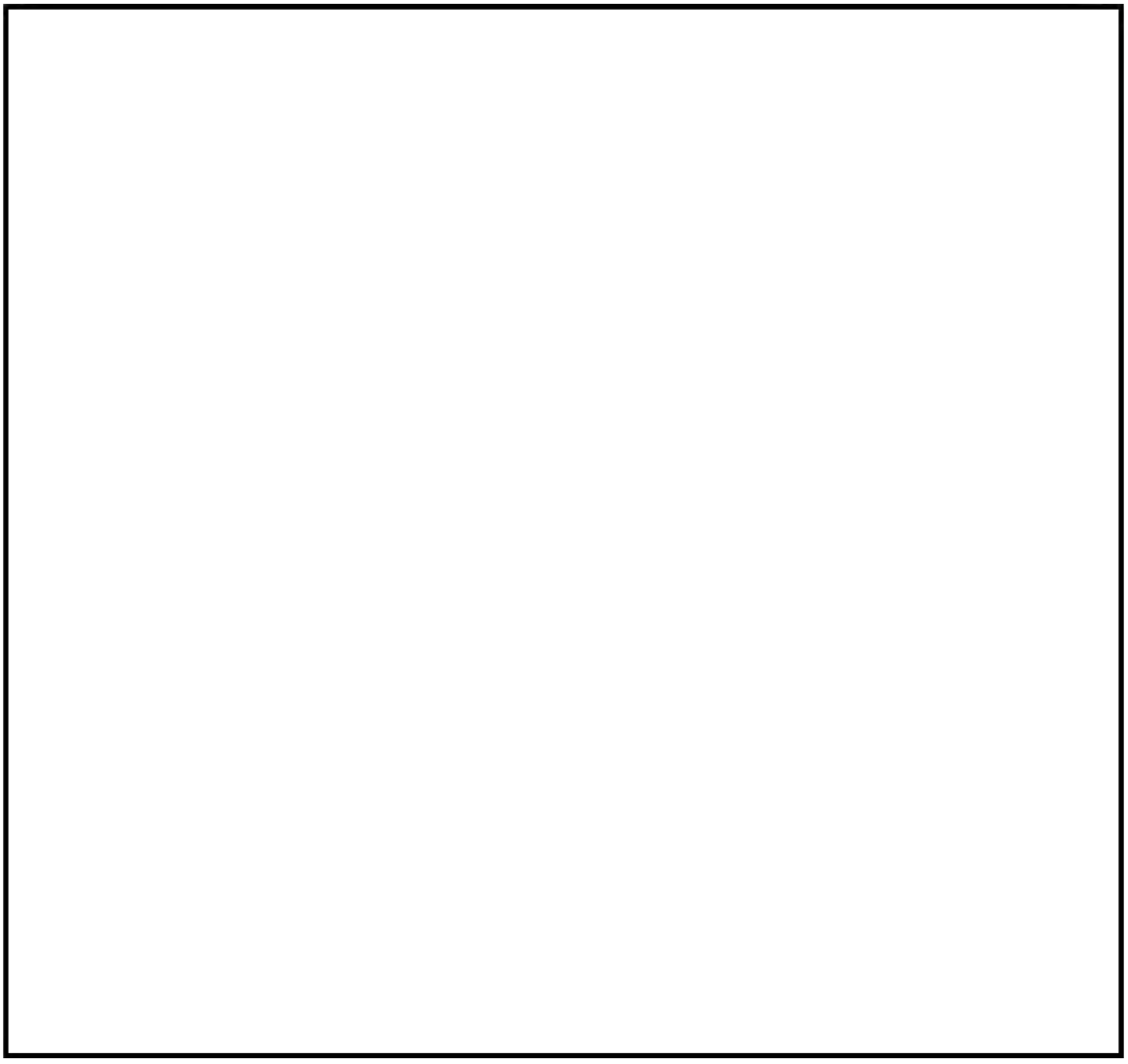
b. Information that is publicly available or does not identify United States persons may be disseminated for any lawful purpose. (U)

c. Dissemination of information provided to the FBI by other Intelligence Community agencies is subject to applicable agreements and understandings with such agencies concerning the dissemination of such information. (U)

b7E
Referral/Consult

2. Department of Justice (U)

a. The FBI may share information obtained through activities under the NSIG with other components of the Department of Justice. (U)



[redacted]

4. Federal Authorities (U)

The FBI may disseminate information obtained through activities under the NSIG to other federal authorities when:

a. the information relates to a crime or other violation of law or regulation which falls within the recipient's investigative jurisdiction, or the information otherwise relates to the recipient's authorized responsibilities;

b. the recipient is a component of the Intelligence Community, and the information is provided to allow the recipient to determine whether the information is relevant to its responsibilities and can be retained or used;

c. the information is required to be furnished to another federal agency by Executive Order 10450 or its successor; or

d. the information is required to be disseminated by statute, Presidential directive, National Security Council directive, Attorney General directive, or interagency agreement approved by the Attorney General. (U)

b7E

2-46 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-47 (U) Disseminating Information to Congressional Committees

A. (U) Members of Congress do not require a determination of eligibility for access to classified information. All other Legislative personnel, however, must be determined eligible by the DOJ Security Officer. See: 28 Code of Federal Regulations Section 17.46(c).

B. (U) Except for briefings and testimony on matters of general intelligence interest, information obtained through activities under the NSIG may be disseminated to the appropriate congressional committees when authorized by the AG or DAG or an official designated by the AG. Other agencies involved in the collection of information will be consulted prior to dissemination to congressional committees. If U.S. person information is to be withheld from dissemination, any decision regarding conflicts over the decision to withhold the information will be referred to the AG, the DAG, or an official designated by the AG for resolution . See Attorney General Guidelines for FBI National Security Investigations Part VII.B.7.

2-48 (U) Disseminating Information to the Federal Judiciary

A. (U) Justices of the U.S. Supreme Court, and Judges of the U.S. Courts of Appeal and District Courts do not require a determination of eligibility for access to classified information. Federal Magistrate Judges and all other Judicial personnel, however, must be determined eligible by the DOJ Security Officer. See: 28 Code of Federal Regulations Section 17.46(c).

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

2-49 (U) Disseminating Information to the White House

A. Information may be shared with the White House (President, Vice President, Assistant to the President for National Security Affairs, the National Security Council, and Homeland Security Council) when (See Attorney General Guidelines for FBI National Security Investigations Part VII.B.8.):

a. Requested by the National Security Council (NSC)

[redacted]

b7E

d. The limitations on dissemination of information by the FBI to the White House under the NSIG do not apply to dissemination to the White House of information acquired in the course of an FBI investigation

requested by theWhite House into the background of a potential employee or appointee, or responses to requests from the White House under Executive Order 10450.

2-50 (U) Disseminating Information to Foreign Governments, and Investigations at their Behest

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-51 (U) Disseminating Information to State and Local Government Agencies

A. (U) Information relating to crimes may be disseminated to State and local governments with appropriate jurisdiction, if such dissemination is consistent with U.S. National Security interests. See: id. Section VII.B.2.b.

1. Information disseminated to State and local government agencies must include statements that the information may be used for evidentiary purposes only with the express written approval of DOJ, after consultation with the FBI.

B. (U) Classified information may not be disseminated to representative of State or local government agencies unless it can be ascertained that they possess appropriate security clearances and have a proper need-to-know. See: Manual of Administrative Operations and Procedures, Section 9-3.1.3.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

2-52 (U) Disseminating Information to the Private Sector

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-53 (U) Data Collection Method for Foreign Counterintelligence, Foreign Intelligence and

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-54 (U) IIIA (Integrated Intelligence Information Application)

b7E

[redacted]

2-55 (U) President's Foreign Intelligence Advisory Board Matters

A. (U) The PFIAB is a body of not more than 16 persons who are not employed by the Government, who are appointed by the President, and who are charged with assessing the quality and adequacy of: (a) intelligence collection, (b) intelligence analyses and estimates, and of (c) foreign counterintelligence and other intelligence activities. It is authorized to review the performance of all agencies within the U.S. Intelligence Community. See: Executive Order 12863, Section 1.2.

1. The PFIAB reports directly to the President; and, to the extent permitted by law, the heads of agencies within the U.S. Intelligence Community must provide it access to all information which it considers necessary for carrying out its responsibilities. See: id. Sections 1.2 and 1.3.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

2-56 (U) Intelligence Oversight Board Matters (Case Identification Number 278-HQ-C1229736-VIO)

Superseded by Corporate Policy Directive #0188D titled, "(U) Guidance on Intelligence Oversight Board Matters," dated 04/22/2009.

Effective Date: 04/22/2009

2-57 (U) Alpha Designations

NFIP File Classifications and Alpha Designations can be found on the Resource Planning Office's (RPO) FBI Classifications website.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 4
Page 4 ~ b1
Page 11 ~ b1
Page 12 ~ b1
Page 24 ~ b7E, Referral/Consult